Legislación Nacional

BUENOS AIRES, 16 ABR 1998BUENOS AIRES, 16 ABR 1998VISTO los Decretos Nros.: 660 del 24 de junio de 1996 y 998 del 30 de agosto de 1996, la Resolución Nº 45 del 17 de marzo de 1997 de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS, yCONSIDERANDO:Que la necesidad de optimizar la actividad de la Administración Pública Nacional adecuando sus sistemas de registración de datos, tendiendo a eliminar el uso del papel y automatizando sus circuitos administrativos, amerita la introducción de tecnología de última generación, entre las cuales se destacan aquellas relativas al uso de la firma digital, susceptible de la misma o superior garantía de confianza que la firma ológrafa.Que la resolución Nº 45 del 17 de marzo de 1997 de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS ha constituido un hito importante en tal dirección, al autorizar su empleo en todo el ámbito del Sector Público Nacional.Que se considera necesario estimular la difusión de las citadas tecnologías a través del dictado de una norma de jerarquía superior, que promueva la extensión del uso de la firma digital a todo el ámbito del Sector Público Nacional.Que la tecnología aquí propuesta ya ha sido incorporada en la legislación de otros países, con positiva repercusión tanto en el ámbito privado como público.Que el mecanismo de la firma digital cumple con la condición de no repudio, por la cual resulta posible probar inequívocamente que una persona firmó efectivamente un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre que su implementación se ajuste a los procedimientos aquí descriptos.Que es indispensable establecer una Infraestructura de Firma Digital para el Sector Público Nacional con el fin de crear las condiciones de un uso confiable del documento suscripto digitalmente.Que la presente normativa fue concebida con el propósito de crear una alternativa válida a la firma ológrafa para el Sector Público Nacional.Que resulta conveniente, en virtud del grado de especialidad alcanzado con la puesta en práctica de la reglamentación del Artículo 49 de la Ley 11.672 (t.o. 1997), que las funciones del Organo Auditante recaigan en la CONTADURIA GENERAL DE LA NACION, dependiente de la SUBSECRETARIA DE PRESUPUESTO de la SECRETARIA DE HACIENDA DEL MINISTERIO DE ECONOMIA Y OBRAS Y SERVICIOS PUBLICOS.Que las disposiciones de la presente normativa complementan las disposiciones del Decreto Nº 333 del 19 de febrero de 1985 y sus modificatorios.Que dada su índole, se ha considerado conveniente y necesario que la autorización del empleo de la tecnología de la firma digital en el ámbito del Sector Público Nacional se sujete a un término de vigencia, que permita evaluar, a partir de su efectiva utilización, tanto su funcionamiento en las diferentes jurisdicciones cuanto el grado de confiabilidad y seguridad del sistema.Que en mérito a tales circunstancias se prevé expresamente en la presente normativa la elaboración, por la Autoridad de Aplicación, de un informe acerca de los resultados del empleo de la firma digital a fin de que, sobre la base de las conclusiones emergentes, la JEFATURA DE GABINETE DE MINISTROS proponga al PODER EJECUTIVO NACIONAL las medidas tendientes a fijar un régimen definitivo en la materia.Que asimismo y con idéntico fundamento, se delega en la JEFATURA DE GABINETE DE MINISTROS la facultad de prorrogar, por una única vez, el plazo del Artículo 1º del presente Decreto.Que la presente medida se dicta en uso de las facultades conferidas por el Artículo 99 inciso 1º de la CONSTITUCION NACIONAL.Por ello,EL PRESIDENTE DE LA NACION ARGENTINADECRETAARTÍCULO 1º.- Autorízase por el plazo de dos años, a contar del dictado de los manuales de procedimiento y de los estándares aludidos en el artículo 6° del presente Decreto, el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa, en las condiciones definidas en la Infraestructura de Firma Digital para el Sector Público Nacional que como Anexo I integra el presente Decreto. En el régimen del presente Decreto la firma digital tendrá los mismos efectos de la firma ológrafa, siempre que se hayan cumplido los recaudos establecidos en el Anexo I y dentro del ámbito de aplicación definido en el artículo 3.ARTÍCULO 2°- Los términos del este reglamento tendrán los alcances definidos en el Glosario que como Anexo II integra el presente Decreto.ARTÍCULO 3º.- Las disposiciones del presente Decreto serán de aplicación en todo el ámbito del Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, Sociedades del Estado, Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera que sea su denominación o naturaleza jurídica, en el que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones.ARTÍCULO 4º.- Los organismos del Sector Público Nacional deberán arbitrar los medios que resulten adecuados para extender el empleo de la tecnología de la firma digital, en función de los recursos con los que cuenten y en el más corto plazo posible.ARTÍCULO 5º - La correspondencia entre una clave pública, elemento del par de claves que permite verificar una firma digital, y el agente titular de la misma, será acreditada mediante un certificado de clave pública emitido por una Autoridad Certificante Licenciada. Los requisitos y condiciones para la vigencia y validez de los certificados de clave pública (emisión, aceptación, revocación, expiración y demás contingencias del procedimiento), así como las condiciones bajo las cuales deben operar las Autoridades Certificantes Licenciadas integrantes de la Infraestructura de

Firma Digital para el Sector Público Nacional, quedan establecidas en el citado Anexo I.ARTÍCULO 6º.- Dispónese que la Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros, sea la Autoridad de Aplicación del presente Decreto, estando facultada, además, para dictar los manuales de procedimiento de las Autoridades Certificantes Licenciadas y de los Organismos Auditante y Licenciante, y los estándares tecnológicos aplicables a las claves, los que deberán ser definidos en un plazo no mayor de CIENTO OCHENTA (180) DIAS corridos, y cuyos contenidos deberán reflejar el último estado del arte. Los organismos del Sector Público Nacional deberán informar a la Autoridad de Aplicación, con la periodicidad que ésta establezca, las aplicaciones que concreten de la tecnología autorizada por el presente Decreto.ARTÍCULO 7º - Dispónese que el presente Decreto establece una alternativa a las estipulaciones pertinentes del Decreto Nº 333 del 19 de febrero de 1985 y sus modificatorios, respecto de los actos alcanzados por el artículo 1°.ARTÍCULO 8º - La Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros cumplirá las funciones de Organismo Licenciante con los alcances definidos en el Anexo I del presente Decreto.ARTÍCULO 9º - La Contaduría General de la Nación, dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos, cumplirá las funciones de Organismo Auditante en los términos de lo establecido en el Anexo I del presente Decreto.ARTÍCULO 10° - Ciento ochenta (180) días corridos antes de la finalización del plazo establecido en el artículo 1°, la autoridad de aplicación definida en el artículo 6 del presente Decreto deberá elaborar y remitir a la Jefatura de Gabinete de Ministros un informe acerca de los resultados que la aplicación del sistema autorizado hubiere tenido en las respectivas jurisdicciones. La Jefatura de Gabinete de Ministros examinará dicho informe y propondrá al Poder Ejecutivo el régimen definitivo a adoptar en la materia.ARTÍCULO 11 - Deléguese en la Jefatura de Gabinete de Ministros la facultad de prorrogar, por una única vez, el plazo establecido en el Artículo 1º del presente Decreto.ARTÍCULO 12º.- Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.DECRETO Nº 427ANEXO IINFRAESTRUCTURA DE FIRMA DIGITALPARA EL SECTOR PUBLICO NACIONALORGANISMO LICENCIANTEFunciones:1. Otorga las licencias habilitantes para acreditar a las autoridades certificantes y emite los correspondientes CERTIFICADOS DE CLAVE PUBLICA, que permiten VERIFICAR LAS FIRMAS DIGITALES de los CERTIFICADOS que éstas emitan;2. Deniega las solicitudes de licencias a las autoridades certificantes que no cumplan con los requisitos establecidos para su autorización;3. Revoca las licencias otorgadas a las AUTORIDADES CERTIFICANTES LICENCIADAS que dejan de cumplir con los requisitos establecidos para su autorización;4. Verifica que las AUTORIDADES CERTIFICANTES LICENCIADAS utilicen sistemas TECNICAMENTE CONFIABLES;5. Considera para su aprobación el manual de procedimientos, el plan de seguridad y el de cese de actividades presentados por las autoridades certificantes;6. Acuerda con el ORGANISMO AUDITANTE el plan de auditoría para las AUTORIDADES CERTIFICANTES LICENCIADAS;7. Dispone la realización de auditorías de oficio;8. Resuelve los conflictos individuales que se susciten entre el SUSCRIPTOR de un CERTIFICADO y la AUTORIDAD CERTIFICANTE LICENCIADA emisora del mismo;9. Resuelve todas aquellas contingencias respecto a la Infraestructura de FIRMA DIGITAL.Obligaciones:En su calidad de SUSCRIPTOR de CERTIFICADO y de autoridad certificante, el ORGANISMO LICENCIANTE tiene idénticas obligaciones que las AUTORIDADES CERTIFICANTES LICENCIADAS, y además debe:1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la CLAVE PRIVADA de cualquier SUSCRIPTOR de los CERTIFICADOS que emita;2. Mantener el control de su propia CLAVE PRIVADA e impedir su divulgación;3. Revocar su propio CERTIFICADO DE CLAVE PUBLICA frente al compromiso de su CLAVE PRIVADA;4. Permitir el acceso público permanente a los CERTIFICADOS DE CLAVE PUBLICA que ha emitido en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS, y a la LISTA DE CERTIFICADOS REVOCADOS, por medio de conexiones de telecomunicaciones públicamente accesibles. Esto también se aplica a la información sobre direcciones y números telefónicos de las AUTORIDADES CERTIFICANTES LICENCIADAS;5. Permitir el ingreso de los funcionarios autorizados del ORGANISMO AUDITANTE a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;6. Publicar su propio CERTIFICADO DE CLAVE PUBLICA en el Boletín Oficial, y en DOS (2) diarios de difusión nacional, durante TRES (3) días consecutivos a partir del día de su emisión;7. Revocar los CERTIFICADOS emitidos en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS incursas en causales de revocación de licencia, o que han cesado sus actividades;8. Revocar los CERTIFICADOS emitidos en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS, cuando las CLAVES PUBLICAS que en ellos figuran dejan de ser TECNICAMENTE CONFIABLES;9. Supervisar la ejecución del plan de cese de actividades de las AUTORIDADES CERTIFICANTES LICENCIADAS que discontinúan sus funciones;10. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.ORGANISMO AUDITANTEFunciones:1. Audita periódicamente al ORGANISMO LICENCIANTE y a las AUTORIDADES CERTIFICANTES LICENCIADAS;2. Audita a las autoridades certificantes previo a la obtención de sus licencias;3. Acuerda con el ORGANISMO LICENCIANTE el plan de auditoría para las AUTORIDADES CERTIFICANTES LICENCIADAS;4. Audita a las

AUTORIDADES CERTIFICANTES LICENCIADAS a solicitud del ORGANISMO LICENCIANTE;5. Efectúa las revisiones de cumplimiento de las recomendaciones formuladas en las auditorías.Obligaciones:El ORGANISMO AUDITANTE debe:1. Utilizar técnicas de auditoría apropiadas en sus evaluaciones;2. Evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del mnual de procedimientos y el plan de seguridad aprobados por el ORGANISMO LICENCIANTE;3. Verificar que se utilicen sistemas TECNICAMENTE CONFIABLES;4. Emitir informes de auditoría con los hallazgos, conclusiones y recomendaciones en cada caso;5. Realizar revisiones de seguimiento de las auditorías, para determinar si el organismo auditado ha tomado las acciones correctivas que surjan de las recomendaciones;6. Emitir informes con las conclusiones de las revisiones de seguimiento de auditorías;7. Intervenir en los simulacros de planes de contingencia;8. Dar copia de todos los informes de auditoría por él emitidos al ORGANISMO LICENCIANTE.AUTORIDAD CERTIFICANTE LICENCIADAFunciones:1. Emite CERTIFICADOS DE CLAVE PUBLICA;Para emitir CERTIFICADOS DE CLAVE PUBLICA, la AUTORIDAD CERTIFICANTE LICENCIADA debe:a) recibir del agente requirente una solicitud de EMISION DE CERTIFICADO DE CLAVE PUBLICA, la cual deberá estar firmada digitalmente con la correspondiente CLAVE PRIVADA;b) verificar fehacientemente la información identificatoria del solicitante, la cual deberá estar siempre incluida en el CERTIFICADO, y toda otra información que según lo dispuesto en el manual de procedimientos de la AUTORIDAD CERTIFICANTE LICENCIADA, deba ser objeto de verificación, lo cual deberá realizarse de acuerdo a lo dispuesto en el citado manual;c) numerar correlativamente los CERTIFICADOS emitidos;d) mantener copia de todos los CERTIFICADOS emitidos, consignando su fecha de emisión.La AUTORIDAD CERTIFICANTE LICENCIADA puede, opcionalmente, incluir en un CERTIFICADO información no verificada, debiendo indicar claramente tal cualidad.2. Revoca CERTIFICADOS DE CLAVE PUBLICA;La AUTORIDAD CERTIFICANTE LICENCIADA revocará los CERTIFICADOS DE CLAVE PUBLICA por ella emitidos:a) por solicitud de su SUSCRIPTOR; ob) por solicitud de un TERCERO; oc) si llegara a determinar que un CERTIFICADO fue emitido en base a una información falsa, que en el momento de la EMISION hubiera sido objeto de verificación; od) si llegara a determinar que las CLAVES PUBLICAS contenidas en los CERTIFICADOS dejan de ser TECNICAMENTE CONFIABLES; oe) si cesa en sus actividades y no transfiere los CERTIFICADOS emitidos por ella a otra AUTORIDAD CERTIFICANTE LICENCIADA;La solicitud de REVOCACION DE UN CERTIFICADO debe hacerse en forma personal o por medio de un DOCUMENTO DIGITAL FIRMADO. Si la revocación es solicitada por el SUSCRIPTOR, ésta deberá concretarse de inmediato. Si la revocación es solicitada por un TERCERO, tendrá lugar dentro de los plazos mínimos necesarios para realizar las verificaciones del caso.La revocación debe indicar el momento desde el cual se aplica y no puede ser retroactiva o a futuro. El CERTIFICADO revocado deberá incluirse inmediatamente en la LISTA DE CERTIFICADOS REVOCADOS, y la lista debe estar firmada por la AUTORIDAD CERTIFICANTE LICENCIADA. Dicha lista debe hacerse pública en forma permanente, por medio de conexiones de telecomunicaciones públicamente accesibles.La AUTORIDAD CERTIFICANTE LICENCIADA debe emitir una constancia de la revocación para el solicitante.3. Provee, opcionalmente, el servicio de SELLADO DIGITAL DE FECHA Y HORA.Obligaciones:Adicionalmente a sus obligaciones emergentes como SUSCRIPTORA de su CERTIFICADO emitido por el ORGANISMO LICENCIANTE, la AUTORIDAD CERTIFICANTE LICENCIADA debe:1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la CLAVE PRIVADA del SUSCRIPTOR;2. Mantener el control de su CLAVE PRIVADA e impedir su divulgación;3. Solicitar inmediatamente la REVOCACION DE SU CERTIFICADO, cuando tuviera sospechas fundadas de que su CLAVE PRIVADA ha sido comprometida;4. Solicitar al ORGANISMO LICENCIANTE la revocación de su CERTIFICADO cuando la CLAVE PUBLICA en él contenida deje de ser TECNICAMENTE CONFIABLE;5. Informar inmediatamente al ORGANISMO LICENCIANTE sobre cualquier cambio en los datos contenidos en su CERTIFICADO, o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo;6. Operar utilizando un sistema TECNICAMENTE CONFIABLE;7. Notificar al solicitante sobre las medidas necesarias que éste está obligado a adoptar para crear FIRMAS DIGITALES seguras y para su VERIFICACION confiable; y de las obligaciones que éste asume por el sólo hecho de ser SUSCRIPTOR de un CERTIFICADO DE CLAVE PUBLICA;8. Recabar únicamente aquellos datos personales del SUSCRIPTOR del CERTIFICADO que sean necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el CERTIFICADO, será de trato confidencial por parte de la AUTORIDAD CERTIFICANTE LICENCIADA;9. Poner a disposición del SUSCRIPTOR de un CERTIFICADO emitido por ésta AUTORIDAD CERTIFICANTE LICENCIADA, toda la información relativa a la tramitación del CERTIFICADO;10. Mantener la documentación respaldatoria de los CERTIFICADOS emitidos por DIEZ (10) años a partir de su fecha de vencimiento o revocación;11. Permitir el acceso público permanente a los CERTIFICADOS que ha emitido, y a la LISTA DE CERTIFICADOS REVOCADOS, por medio de conexiones de telecomunicaciones públicamente accesibles;12. Publicar su dirección y sus números telefónicos;13. Permitir el ingreso de los funcionarios autorizados del

ORGANISMO LICENCIANTE o del ORGANISMO AUDITANTE a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;14. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.Cese de Actividades:Los CERTIFICADOS emitidos por una AUTORIDAD CERTIFICANTE LICENCIADA que cesa en sus funciones se revocarán a partir del día y la hora en que cesa su actividad, a menos que sean transferidos a otra AUTORIDAD CERTIFICANTE LICENCIADA. La AUTORIDAD CERTIFICANTE LICENCIADA notificará mediante la publicación por TRES (3) días consecutivos en el Boletín Oficial, la fecha y hora de cese de sus actividades, que no podrá ser anterior a los NOVENTA (90) días corridos contados desde la fecha de la última publicación. La notificación también deberá hacerse individualmente al ORGANISMO LICENCIANTE.Cuando se hayan emitido CERTIFICADOS a personas ajenas al Sector Público Nacional, la AUTORIDAD CERTIFICANTE LICENCIADA publicará durante TRES (3) días consecutivos en uno o más diarios de difusión nacional, el cese de sus actividades.La AUTORIDAD CERTIFICANTE LICENCIADA podrá disponer de medios adicionales de comunicación del cese de sus actividades a los SUSCRIPTORES de CERTIFICADOS que son ajenos al Sector Público Nacional.Si los CERTIFICADOS son transferidos a otra AUTORIDAD CERTIFICANTE LICENCIADA, toda la documentación pertinente también deberá ser transferida a ella.Requisitos para obtener la licencia de autoridad certificante:La autoridad certificante que desee obtener una licencia deberá:1. Presentar una solicitud;2. Contar con un dictamen favorable emitido por el ORGANISMO AUDITANTE;3. Someter a aprobación del ORGANISMO LICENCIANTE el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;4. Emplear para el ejercicio de las actividades de certificación, personal técnicamente idóneo y que no se encuentre incurso en los supuestos de inhabilitación para desempeñar funciones dentro del Sector Público Nacional;5. Presentar toda otra información relevante al proceso de otorgamiento de licencias que sea exigida por el ORGANISMO LICENCIANTE.SUSCRIPTOR DE CERTIFICADO DE CLAVE PUBLICAObligaciones del SUSCRIPTOR:El SUSCRIPTOR de un CERTIFICADO DE CLAVE PUBLICA debe:1. Proveer todos los datos requeridos por la AUTORIDAD CERTIFICANTE LICENCIADA bajo declaración jurada;2. Mantener el control de su CLAVE PRIVADA e impedir su divulgación;3. Informar inmediatamente a la AUTORIDAD CERTIFICANTE LICENCIADA, sobre cualquier circunstancia que pueda haber comprometido su CLAVE PRIVADA;4. Informar inmediatamente a la AUTORIDAD CERTIFICANTE LICENCIADA cuando cambie alguno de los datos contenidos en el CERTIFICADO que hubieran sido objeto de verificación.CERTIFICADOS DE CLAVE PUBLICAContenido del CERTIFICADO DE CLAVE PUBLICA:El CERTIFICADO DE CLAVE PUBLICA contendrá, como mínimo, los siguientes datos:1. Nombre del SUSCRIPTOR del CERTIFICADO;2. Tipo y número de documento del SUSCRIPTOR del CERTIFICADO, o número de licencia, en el caso de CERTIFICADOS emitidos para AUTORIDADES CERTIFICANTES LICENCIADAS;3. CLAVE PUBLICA utilizada por el SUSCRIPTOR;4. Nombre del algoritmo que debe utilizarse con la CLAVE PUBLICA en él contenida ;5. Número de serie del CERTIFICADO;6. PERIODO DE VIGENCIA del CERTIFICADO;7. Nombre de la AUTORIDAD CERTIFICANTE LICENCIADA emisora del CERTIFICADO;8. FIRMA DIGITAL de la AUTORIDAD CERTIFICANTE LICENCIADA que emite el CERTIFICADO, identificando los algoritmos utilizados.9. Todo otro dato relevante para la utilización del CERTIFICADO, se explicitará en el manual de procedimientos de la AUTORIDAD CERTIFICANTE LICENCIADA emisora.Condiciones de Validez del CERTIFICADO DE CLAVE PUBLICA:El CERTIFICADO DE CLAVE PUBLICA es válido únicamente si:1. ha sido emitido por una AUTORIDAD CERTIFICANTE LICENCIADA;2. no ha sido revocado;3. no ha expirado.ANEXO IIGLOSARIOAUTORIDAD CERTIFICANTE LICENCIADALICENCIADA:Organo administrativo que emite que emite CERTIFICADOS DE CLAVE PUBLICA.CERTIFICADO o CERTIFICADO DE CLAVE PUBLICA: o CERTIFICADOSDOCUMENTO DIGITAL emitido y firmado digitalmente por una AUTORIDAD CERTIFICANTE LICENCIADA, que asocia una CLAVE PUBLICA con su SUSCRIPTOR durante el dentro del PERIODO DE VIGENCIA del CERTIFICADO, y que asimismo hace plena prueba dentro de la Administración Sector Público Nacional, de la veracidad de su contenido.CLAVE PRIVADA:En un CRIPTOSISTEMA ASIMETRICO, es aquella que se utiliza para firmar digitalmente crear una FIRMA DIGITAL.CLAVE PUBLICA:En un CRIPTOSISTEMA ASIMETRICO, es aquella que se utiliza para verificar una FIRMA DIGITAL.COMPUTACIONALMENTE NO FACTIBLE:Dícese de aquellos cálculos matemáticos asistidos por computadora que para ser llevados a cabo requieren de tiempo y recursos informáticos que superan ampliamente a los disponibles en la actualidad.CORRESPONDER:Con referencia a un cierto PAR DE CLAVES, significa pertenecer a dicho par.CRIPTOSISTEMA ASIMETRICO:Algoritmo que utiliza un PAR DE CLAVES, una CLAVE PRIVADA para firmar digitalmente y su correspondiente CLAVE PUBLICA para verificar esa FIRMA DIGITAL, cuya CLAVE PRIVADA crea una FIRMA DIGITAL, y cuya correspondiente CLAVE PÚBLICA se utiliza para VERIFICAR esa FIRMA DIGITAL. A efectos de este Decreto, se entiende que el CRIPTOSISTEMA ASIMETRICO deberá ser TECNICAMENTE CONFIABLE.DIGESTO SEGURO (Hash Result):La secuencia de bits de longitud fija resultado producido por una FUNCION DE DIGESTO SEGURO luego de procesar un

DOCUMENTO DIGITAL.DOCUMENTO DIGITAL:Representación digital de actos, hechos o datos jurídicamente relevantes.DOCUMENTO DIGITAL FIRMADO:DOCUMENTO DIGITAL al cual se le ha aplicado una FIRMA DIGITAL.EMISION DE UN CERTIFICADO:La creación de un CERTIFICADO por parte de una AUTORIDAD CERTIFICANTE LICENCIADA.ORGANISMO AUDITANTE:Organo administrativo encargado de auditar la actividad del ORGANISMO LICENCIANTE y de las AUTORIDADES CERTIFICANTES LICENCIADAS.ORGANISMO LICENCIANTE:Organo administrativo encargado de otorgar las licencias a las autoridades certificantes y de supervisar la actividad de las AUTORIDADES CERTIFICANTES LICENCIADAS.FIRMA DIGITAL:Resultado de una transformación de un DOCUMENTO DIGITAL empleando un CRIPTOSISTEMA ASIMETRICO y un DIGESTO SEGURO, de forma tal que una persona que posea el DOCUMENTO DIGITAL inicial y la CLAVE PUBLICA del firmante pueda determinar con certeza :1. Si la transformación se llevó a cabo utilizando usando la CLAVE PRIVADA que corresponde a la CLAVE PUBLICA del firmante, lo que impide su repudio2. Si el DOCUMENTO DIGITAL ha sido modificado desde que se efectuó la transformación, lo que garantiza su integridad.La conjunción de los dos requisitos anteriores garantiza su NO REPUDIO y su INTEGRIDAD.FUNCION DE DIGESTO SEGURO:Es una función matemática que transforma un DOCUMENTO DIGITAL en una secuencia de bits de longitud fija, llamada DIGESTO SEGURO, de forma tal que:- Se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo DOCUMENTO DIGITAL; - Es COMPUTACIONALMENTE NO FACTIBLE inferir o reconstituir un DOCUMENTO DIGITAL a partir de su DIGESTO SEGURO; - Es COMPUTACIONALMENTE NO FACTIBLE encontrar dos DOCUMENTOS DIGITALES diferentes que produzcan el mismo DIGESTO SEGURO. INTEGRIDAD:Condición de no alteración de un DOCUMENTO DIGITAL.LISTA DE CERTIFICADOS REVOCADOS:Es la lista publicada por la AUTORIDAD CERTIFICANTE LICENCIADA, de los CERTIFICADOS DE CLAVE PUBLICA por ella emitidos cuya vigencia ha cesado antes de su fecha de vencimiento, por acto revocatorio.NO REPUDIO:Cualidad de la FIRMA DIGITAL, por la cual su autor no puede desconocer un DOCUMENTO DIGITAL que él ha firmado digitalmente.PAR DE CLAVES:CLAVE PRIVADA y su correspondiente CLAVE PUBLICA en un CRIPTOSISTEMA ASIMETRICO, tal que la CLAVE PUBLICA puede verificar una FIRMA DIGITAL creada por la CLAVE PRIVADA.PERIODO DE VIGENCIA (de un CERTIFICADO):Período durante el cual el SUSCRIPTOR puede firmar DOCUMENTOS DIGITALES utilizando la CLAVE PRIVADA correspondiente a la CLAVE PUBLICA contenida en el CERTIFICADO, de modo tal que la FIRMA DIGITAL no sea repudiable.El PERIODO DE VIGENCIA de un CERTIFICADO comienza en la fecha y hora en que fue emitido por la AUTORIDAD CERTIFICANTE LICENCIADA, o en una fecha y hora posterior si así lo especifica el CERTIFICADO, y termina en la fecha y hora de su vencimiento o revocación.PUBLICARDar a conocer, notificar o comunicar por cualquier medio.REVOCACION DE UN CERTIFICADO:Acción de dejar sin efecto en forma permanente un CERTIFICADO a partir de una fecha cierta, incluyéndolo en la LISTA DE CERTIFICADOS REVOCADOS dándolo a publicidad.SELLADO DIGITAL DE FECHA Y HORA:Acción mediante la cual la AUTORIDAD CERTIFICANTE LICENCIADA adiciona la fecha, hora, minutos y segundos (como mínimo) de su intervención, a un DOCUMENTO DIGITAL o a su DIGESTO SEGURO. La información resultante del proceso antes descripto será firmada digitalmente por la AUTORIDAD CERTIFICANTE LICENCIADA.SISTEMA CONFIABLE (Analizar junto con Técnicamente CONFIABLE):Equipos de computación, software y procedimientos relacionados que:1. Sean razonablemente confiables para resguardar contra la posibilidad de intrusión o de uso indebido;2. Brinden un grado razonable de disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;3. Sean razonablemente aptos para el desempeño de sus funciones específicas;4. Cumplan con los requisitos de seguridad generalmente aceptados.SUSCRIPTOR:Persona:- A cuyo nombre se emite un CERTIFICADO, y - Que es titular de la CLAVE PRIVADA correspondiente a la CLAVE PUBLICA incluida en dicho CERTIFICADO.TECNICAMENTE CONFIABLEDícese de los SISTEMAS CONFIABLES que cumplen con los estándares tecnológicos que al efecto dicte la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros.Respecto de las longitudes de claves a utilizar, se requerirá como mínimo una cantidad de bits igual o superior al doble de la longitud de las claves que se puedan quebrar al momento de (generar el PAR DE CLAVES, o crear la FIRMA DIGITAL, o VERIFICAR la FIRMA DIGITAL).Respecto de las longitudes de digestos de DOCUMENTO DIGITAL a utilizar, se requerirá como minimo una cantidad de bits igual o superior al doble de la longitud de digestos de DOCUMENTO DIGITAL que se puedan quebrar al momento de (generar el PAR DE CLAVES, o crear la FIRMA DIGITAL, o VERIFICAR la FIRMA DIGITAL).TERCERO:El que ostenta un derecho subjetivo o interés legítimo .VERIFICACION DE UNA FIRMA DIGITAL:En relación a un DOCUMENTO DIGITAL, una FIRMA DIGITAL, el correspondiente CERTIFICADO DE CLAVE PUBLICA y una LISTA DE CERTIFICADOS REVOCADOS, es la determinación fehaciente de que:- El DOCUMENTO DIGITAL fue firmado digitalmente con la FIRMA DIGITAL fue creada en base por la CLAVE PRIVADA correspondiente a la CLAVE PUBLICA incluida en el CERTIFICADO; - El DOCUMENTO DIGITAL no fue alterado desde que fue firmado

digitalmente.Para aquel documento cuya naturaleza pudiera exigir la necesidad de certificación de fecha cierta, o bien ésta fuere conveniente dado sus efectos, deberá determinarse adicionalmente que el mismo fue firmado digitalmente durante el PERIODO DE VIGENCIA del correspondiente CERTIFICADO